

16
17. The method of claim 15 in which said identification data is a serial number index into a registry database containing names and contact information for proprietors identified by said identification data.

17
18. The method of claim 17 in which the empirical data sets include image data, and the method includes:
converting said image data to pixel form, if not already in said form; and
performing a plurality of statistical analyses on said pixel form image data to discern the identification data therefrom.

18
19. The method of claim 18 in which each statistical analysis includes analyzing a collection of spaced apart pixels to decode a single, first bit of the identification data therefrom, said analysis to decode the first bit encompassing not just said spaced apart pixels, but also pixels adjacent thereto, said adjacent pixels not being encoded with said first bit. --

REMARKS

After entry of the foregoing amendments, claims 2-19 are pending in the application.

A Supplemental Declaration is submitted herewith, claiming priority to several prior applications. The *Related Applications* paragraph of the specification has been amended accordingly.

The Background discussion of the specification has been rewritten to better conform to the subject matter of the amended claims.

Claims 12-19 are newly added; each depends from claim 11. The limitations in these claims are copied from dependent claims 3-10 earlier examined.

Discussion of Technology

The present technology addresses the uncontrolled distribution of imagery, and other creative properties, on the internet.

Presently, photographers and graphic artists publish their works on the internet at their peril. It is trivially simple for any viewer of such works to copy the imagery and, *e.g.*, post it to their own web site.

Given the tremendous extent of computers on the internet, such piracy of creative content goes largely undetected. Only by happenstance does the proprietor of creative content locate such copies.

The present invention addresses this problem. While the preferred embodiment does not prevent the initial copying of the image, it enables image proprietors to locate web sites to which their images have been posted. A report is periodically provided to content owners detailing where their works were found. The owners can then take whatever action is appropriate in the circumstances.

Playboy is the classic example of an image proprietor whose imagery is frequently copied and reposted. Although it has been hesitant to publish its works in digital form – fearing copying – its paper centerfolds have been scanned-in by countless individuals, and the resulting digital imagery posted to the hundreds of unauthorized worldwide web sites.

To counter this piracy, Playboy and other image proprietors have subscribed to a service (MarcSpider) offered by the present assignee (Digimarc) which practices the claimed invention. Day and night a search computer examines thousands of images on the internet, briefly checking each for the possible existence of a watermark. Images that appear to have a watermark are further examined and, if a watermark is present, the encoded data is extracted and the proprietor identified through a database. The image proprietor is informed of the discovery of the image, and the internet address at which it is located. Hundreds of pirated images have been found in the few months that the MarcSpider service has been in operation.

Attached are press accounts reporting Playboy's adoption of the claimed Digimarc technology. Included are the following:

- CNNfn, "Watermarking Copyrights," July 9, 1997;
- Forbes Digital, "Copywrongs," September 5, 1997;
- Wired News, "*Playboy* Hopes 'Watermarks' Keep Bunnies Safe," June 30, 1997;
- NewMedia, "Corralling Your Content," October 13, 1997.

Powell

Powell discloses a method and system for creating digital image signatures. Applicant respectfully submits that Powell does not teach the claimed combinations.

Powell does not appear to disclose the automatic downloading of data, including empirical data sets, from a plurality of computer sites over the internet. The internet is not referenced in Powell. Moreover, nothing indicates any *automatic* downloading, or any downloading. (*Automatic* is in contrast with manually specifying each data set to be downloaded.)

Powell page 2, lines 8-13 is understood to teach simply that images can be distributed in print and electronic form. Page 3, lines 21-34 is understood to review how a print image can be converted to digital form with a scanner. The scanner output can be stored on a diskette for displaying later at a remote site.

Nor does Powell appear to disclose automatic screening of each of plural empirical data sets obtained by the downloading operation, to identify the potential presence of identification data steganographically embedded therein.

Page 5, lines 15-50, is understood to disclose how a suspect image can be normalized preparatory to performing a watermark analysis. Such an operation does not "identify the potential presence of identification data."

Powell teaches the discerning of identification data from a suspect image. However, this operation is not performed on plural images. Nor is it performed on images that have first

passed a screening operation. The cited excerpt at page 5, line 51 through page 6, line 14, is not understood to teach any of these latter elements.

Finally, Powell is not understood to teach generating a report identifying steganographically encoded empirical data sets identified as above, and the site from which each was downloaded.

Page 2, lines 8-23, describes the Background of the Powell work, and reviews the need for a marking technology that allows the proprietor of an image to confirm that a suspect image is derived from his work – a marking that can withstand various modifications. Page 5, lines 12-18, briefly reviews the steps of normalizing a suspect image, and analyzing same to extract any embedded data.

In view of these and other failings of Powell, claim 2 is not anticipated by such art and should be in condition for allowance.

Claims 3-10 all depend from claim 2 and should similarly be allowable. Each is also patentable independent from claim 2.

For example, claim 3 defines a method employing a master code signal that is used in discerning the steganographically encoded identification data from the screened empirical data sets. No master code signal is disclosed in Powell.

The excerpt at page 5, line 36, through page 6, line 14, is understood to teach how to normalize the brightness, contrast and/or color of the suspect image to conform to that of the original image, by reference to the brightness/contrast/color of selected pixels in the original image. Once normalized, the suspect image is subtracted from the original image to identify changes to the Powell's "signature points." (Or the suspect image can be compared with the signed image to determine whether the changes to the signature points match.)

Claim 3 also indicates that one master code signal is used to discern steganographically encoded data from "a plurality" of the screened data sets. Thus, if the locations of Powell's signature points were somehow regarded as a master code signal, those locations are unique to

that image, and are not uniformly applied to all of a plurality of images downloaded from the internet.

Claim 4 specifies that the master code signal has the appearance of unpatterned snow if represented in the pixel domain. Figs. 2, 3 and 5 are not understood to disclose this feature. Figs. 2 and 5, for example, show a sample digital image (page 2, line 54 - page 3, line 2), not a master code signal. Moreover, the image is clearly patterned, showing a head in profile. Similarly, Fig. 3 shows pixel values corresponding to an image excerpt, not an unpatterned master code signal.

Claim 5 specifies that the discerning of the identification data is accomplished without previous knowledge of the audio, image, or video information represented thereby.

Powell teaches just the opposite. In order for Powell to decode a suspect image, he must have either (1) the original (unsigned) image, or (2) the originally signed image. This is evident from the excerpt cited in the Action.

Claim 6 defines a method that includes identifying proprietors of empirical data sets by reference to identification data discerned therefrom, and reporting to said proprietors the sites from which their data sets were downloaded.

Powell teaches that a binary number between 16 and 32 bits in length is encoded into an image (page 3, lines 46-47). However, this number does not allow the proprietor of the image to be identified. Rather, it allows *the proprietor* of the work to *confirm* that the image is his own.

Powell contemplates that the person analyzing the suspect image is its proprietor -- analysis requires access to the original (unsigned) image, or the originally-signed image. A person who did *not* already know the identity of the proprietor wouldn't know where to look in the image for signature points. Thus, Powell's binary number simply serves as an arbitrary hallmark whose presence in a suspect image cannot be simply disregarded as happenstance.

Still further, nothing in Powell teaches "reporting to said proprietors the sites from which their empirical data sets were downloaded.

Claim 7 defines a method that includes encoding information *in addition* to data identifying the proprietor. Since Powell's binary number is an arbitrary tag that allows a suspect and an original image to be correlated, no additional data is represented thereby.

Claim 8 defines a method in which the identification data is a serial number index into a registry database containing names and contact information for proprietors identified by the identification data.

As noted, Powell's binary number is an arbitrary marking. However, apart from this distinction, Powell also does not teach use of his encoded number as an index into a registry database containing names and contact information.

Claim 9 defines a method in which the discerning operation includes performing a plurality of statistical analyses on the pixel-form image. Powell employs a deterministic detection method in which the outcome is based on the values of a few specific pixels. He does not teach an arrangement in which the embedded information is discerned as the result of plural statistical analyses, each of which relies on statistical characteristics of the image.

Claim 10 further defines the statistical analysis as including analyzing a collection of spaced apart pixels to decode a single, first bit of the identification data, said analysis encompassing not just the spaced apart pixels, but also pixels adjacent thereto, where the adjacent pixels are not encoded with that first bit.

Powell does not teach such an arrangement.

Powell may be interpreted as examining a collection of spaced apart pixels to decode a first bit, because he teaches that each bit may be redundantly encoded at several different locations.

However, that analysis by Powell does not meet the further limitation of claim 10, namely that the analysis to decode the first bit encompasses "not just the spaced apart pixels, but also pixels adjacent thereto, said adjacent pixels not being encoded with said first bit." Powell, in contrast, examines the values just at the "signature point" pixels; the tapering of pixel values therearound is to reduce the human visibility of artifacts of the encoding.

Moreover, the pixels adjacent Powell's signature points are encoded in accordance with the *same* bit with which the signature bit is encoded (being changed in proportionately tapered fashion) – again contrary to the claim's requirement.

Claim 11 defines a method for surveying distribution of proprietary empirical data sets on computer sites accessible via the internet. Again, Powell does not mention the internet, nor any method or surveying distribution of proprietary material on computer sites accessible via the internet.

Claim 11 further requires provision of a master code signal useful for detecting steganographic coding within empirical data sets. The claimed master code signal is employed with each of "a plurality" of empirical data sets.

As discussed above in connection with claim 3, Powell has no disclosure of such a master code signal useful for detecting steganographic coding within plural empirical data sets.

Claim 11 further requires automatic downloading of data, including empirical data sets, from a plurality of computer sites over the internet. Again, as discussed above in connection with claim 2, Powell does not teach such an arrangement.

Claim 11 further requires – for each of plural empirical data sets obtained by said downloading operation – discerning certain identification data, if any, steganographically encoded therein, said discerning employing said master code signal as a decoding key.

Again, as discussed previously, Powell makes no use of a single master code signal as a decoding key for plural sets of empirical data.

Claim 11 further requires generating a report identifying steganographically encoded empirical data sets identified by the foregoing steps, and the site from which each was downloaded. Again, as discussed above, Powell does not generate a report. He does not download data. He does not detail which site contained which empirical data.

In view of these and other failings of Powell, claim 11 is not anticipated by such art and should be in condition for allowance.

Claims 12-20 are allowable for the reasons discussed above in connection with claims 2-10.

Stefik

(Applicant's priority claim has been amended to claim priority to three parent applications pre-dating Stefik (Application Nos. 08/154,866, 08/215,289, and 08/327,426). Without waiving their priority rights, applicant details below certain of the differences between Stefik and the claimed combinations.)

Stefik is understood to disclose a rights-management system which limits the uses to which digital works can be put. Stefik addresses different concerns than the claimed combinations, using different methods.

Stefik *distributes* digital data (6:19). The claimed combinations do not. Rather, they *track* where such digital data has been spread by third parties.

Stefik *limits access* to digital data. The claimed combinations do not. It is the *unlimited* access to images, etc., provided by the internet that is one of the motivations for the claimed combinations.

Stefik limits the actions that can be performed on digital data (*e.g.* 4:2, 21:13). The claimed combinations do not.

Stefik stores his digital data only in known, "trusted repositories" (*e.g.* 6:57:61; 8:6-7; 12:40 - 13:1-66). The claimed combinations, in contrast, can track down digital data from unknown locations.

Stefik's associated data (*e.g.* "usage rights") are not hidden. The claimed combinations, in contrast employ *steganographic* encoding (*i.e.* hidden). (Stefik appears to contemplate steganographic encoding of certain "tracer information" in works that are printed onto paper, so that photocopies thereof may be detected. *See* 48:1-26).

Stefik's usage rights are not encoded *within* the content (*e.g.* within pixels representing an image) but are separately represented by a usage grammar associated with the content.

More particularly, Stefik employs descriptor blocks (d-blocks) to characterize content (See Fig. 7). In Fig. 11, for example, d-block 1103 characterizes the third article in a digital magazine. The d-block gives the title of the work ("Article 3"), the starting address of the article, and its length. These addresses refer to the storage location at which the underlying magazine content is stored. The d-block next includes the "Rights Portion" which defines permissible uses of the work. Parent and child pointers follow.

The textual content of the magazine article is not included in the d-block with the usage rights information, etc. Instead, it is separately encoded (see Fig. 6).

Thus, Stefik separates this auxiliary data from the content (10:36-38).

In contrast, the identification data in the claimed combinations is encoded *in* the empirical data set (i.e. *within* the audio, video or image data).

With this by way of background, it can be seen that Stefik does not teach the combinations claimed.

As to claim 2, Stefik does not survey distribution of audio, image, or video data on computer sites accessible via the internet. He distinguishes such systems and instead teaches that trusted repositories -- that are not generally accessible -- should exclusively be used (12:58-61).

Stefik does not teach downloading data, including empirical data sets, from a plurality of computer sites over the internet. Rather, he contemplates that a user will download data from a trusted repository, and then only if the user has been granted proper rights, and then only if the requested data can be downloaded for the purpose requested.

Stefik does not teach any screening of empirical data obtained by a downloading operation to identify the potential presence of identification data steganographically encoded therein. He does not screen, and he does not concern himself with steganographically encoded data. (The cited excerpt at 26:38-46 is understood to disclose various transactions that may be invoked at the Repository when a user requests access to a digital work. None involves screening candidate empirical data sets.)

Stefik does not discern steganographically encoded identification data from each of plural sets of empirical data screened by the screening operation. As noted, the encoding of usage rights, etc., is done separately from the content itself, and in an overt manner, rather than hidden (i.e. steganographic).

Finally, Stefik does not generate a report identifying steganographically encoded empirical data sets identified by the foregoing steps, and the site from which each was downloaded. (The cited excerpt at 17:1-67 is understood to disclose Stefik's Credit Server, on which financial transactions associated with use of digital works are performed.)

Stefik likewise fails to teach the combinations defined by claims 3-10 dependent from claim 2.

Turning to claim 11, Stefik again does not teach a method for surveying distribution of proprietary empirical data sets on computer sites accessible via the internet, as discussed above in connection with claim 2.

Nor does he provide a master code signal useful for detecting steganographic coding within empirical data sets. (The excerpt at 26:38-46 is understood to disclose various transactions that may be invoked at the Repository when a user requests access to a digital work. None involves a master code signal or steganographic decoding.)

Stefik does not teach automatically downloading data, including empirical data sets, from a plurality of computer sites over the internet, as discussed above in connection with claim 2.

Stefik does not teach – for each of plural sets of empirical data obtained by the downloading operation – discerning certain identification data, if any, steganographically encoded therein, said discerning employing the master code signal as a decoding key.

Nor does Stefik teach generating a report identifying steganographically encoded empirical data sets identified by the foregoing steps, and the site from which each was downloaded, as discussed above in connection with claim 2.

In view of these and other failings of Stefik, the claims are believed allowable over such art.

Other Art

The undersigned has briefly reviewed the additional art referenced in the Action. None appears to provide the above-described advantages afforded by the presently claimed combinations (except applicant's own prior patent, which is not prior art).

Information Disclosure Statements

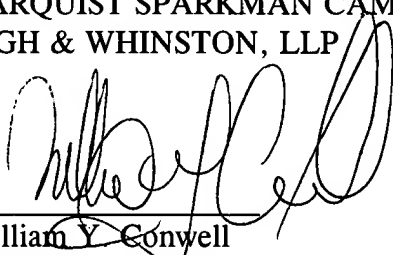
Applicant earlier cited various art, but did not submit same since it was of record in a previously-claimed parent application. The Examiner noted that such art was not readily available to him.

In accordance with the Examiner's request, under separate cover are copies of the earlier-cited references and duplicate Forms PTO-1449 listing same.

Favorable consideration and passage to issue is requested.

Respectfully submitted,

KLARQUIST SPARKMAN CAMPBELL
LEIGH & WHINSTON, LLP

By 
William Y. Conwell
Registration No. 31,943

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
cc: Geoff Rhoads